

Release Notes:

Version WT.01.33 Software

*for HP ProCurve Wireless Edge Services zl Module (J9051A) and
Redundant Wireless Services zl Module (J9052A)*

These release notes include information on the following:

- Downloading software and documentation from the Web ([page 1](#))
- Important Support Notes and Clarifications for each release ([page 4](#))
- A listing of enhancements in each release ([page 16](#))
- A listing of software fixes included in each release ([page 18](#))
- Known software issues and limitations ([page 28](#))

Changes to Dynamic Frequency Selection (DFS) in the 5 GHz Band

Depending on your country/region settings on this product, the available channels in the 5 GHz band may have changed.

Customers in the U.S.

Effective July 20, 2007, new FCC regulations on the use of the 5GHz band, the band used by radios supporting the IEEE 802.11a standard, prohibit the sale of radios not meeting the new specifications. To comply with these new requirements, several channels in the ProCurve Radio Ports 220 (J9005A), and 230 (J9006A) are disabled when using this product (zl Module).

This product disables channels 52, 56, 60, 64 (5.25-5.35 GHz) in the U.S. These channels remain available for use in other countries except as noted below.

Customers in the European Union and Selected Countries/Regions*

In the European Union and selected countries/regions*, ProCurve Wireless Edge Services Modules, Access Points and Radio Ports purchased after April 1, 2008, are subject to new radar interference requirements that limit the available channels in the 5 GHz band. To comply with these new requirements, the operating channels impacted by this change have been removed.

The factory-installed software version that ships with your product limits the available 5 GHz channels to 36, 40, 44 and 48 (5.150 – 5.250 GHz).

* Other countries/regions that apply include South Africa, Turkey, Morocco, Croatia.

Software Update Notice

Updating from Version WT.01.03 to any newer version

When updating a module that is in a redundancy group, the module may fail to rejoin the group if a *non-default* Heartbeat Period was configured for the group. See “Known software issues and limitations” ([page 28](#)).

© Copyright 2007-2010 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

Publication Number

Part Number 5991-8624
May 2010

Applicable Product

ProCurve Wireless Edge Services zl Module(J9051A)
ProCurve Redundant Wireless Services zl Module(J9052A)

Trademark Credits

Microsoft®, Windows®, and Windows NT® are US registered trademarks of Microsoft Corporation.
Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.
Java™ is a US trademark of Sun Microsystems, Inc.

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the *Software License, Warranty and Support* booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Contents

Software Management

Software Updates	1
Downloading Software and Documentation from the Web	1
Downloading Software to the Module	2
Saving Configurations	2
Saving the Current Configuration as the Start-Up Configuration	2
ProCurve Software Code Designations	3

Support Notes and Clarifications

Release WT.01.03	4
Accessing the Web Browser Interface — In Case of Difficulty	4
Configuring Authentication for Web-Users	12
Special Characters for the ACL ID Field	13
Correction: SNMP v3 Default Password	13
Clarification: For Layer 3 Adoption, DHCP Server Option 189 Requires Value Type ‘String’	13
Correction: Stations per Module in a Layer 3 Mobility Domain	13
Correction: Disabling TKIP Countermeasures	13
Clarification: Setting Intrusion Detection with TKIP Countermeasures	14
Release WT.01.13	14
Release WT.01.15	14
Release WT.01.28	14
Logging Aggregation Time	14
Wireless Station Intrusion Detection Configuration	15

Enhancements

Release WT.01.03 Enhancements	16
Features	16
Capabilities	17
Release WT.01.13 Enhancements	17
Support for Client Location Confidence in ProCurve Mobility Manager	17
Release WT.01.17 Enhancements	17
Release WT.01.20 Enhancements	17

Software Fixes

Release WT.01.03	18
Release WT.01.10	18
Release WT.01.13	18
Release WT.01.14	19
Release WT.01.15	19

Contents

Release WT.01.16 19

Release WT.01.17 20

Release WT.01.18 20

Release WT.01.19 20

Release WT.01.20 20

Release WT.01.21 21

Release WT.01.22 22

Release WT.01.23 22

Release WT.01.24 22

Release WT.01.25 22

Release WT.01.26 22

Release WT.01.27 23

Release WT.01.28 24

Release WT.01.29 24

Release WT.01.30 25

Release WT.01.31 26

Release WT.01.32 26

Release WT.01.33 27

Known Software Issues and Limitations

Release WT.01.03 28

Release WT.01.10 33

Release WT.01.13 33

Release WT.01.28 34

Software Management

Software Updates

Check the HP ProCurve Networking Web site frequently for free software updates for the various ProCurve products you may have in your network.

Downloading Software and Documentation from the Web

You can download software updates and the corresponding product documentation from HP ProCurve Networking's Web site as described below.

To Download a Software Version:

To obtain software updates, go to the HP ProCurve Networking Web site at:

www.hp.com/go/procurve/software

and click on **Wireless services modules**.

To Download Product Documentation:

You will need the Adobe® Acrobat® Reader to view, print, and/or copy the product documentation.

To view or download the latest available documentation, go to the HP ProCurve Networking Web site at:


www.hp.com/go/procurve/manuals

and select the desired product.

Note

Documentation for this product may be found on the **Manuals** pages for the following products:

- ProCurve Switch 8200zl series
- ProCurve Switch 5400zl series
- J9051A ProCurve Wireless Edge Services zl Module
- J9052A ProCurve Redundant Wireless Services zl Module

On the resulting Web page, double-click on a document you want. When the document file opens, click on the disk icon  in the Acrobat® toolbar and save a copy of the file.

Downloading Software to the Module

Caution

The startup-config file generated by the latest software release is compatible with the same file generated by earlier software releases. HP recommends that you backup your current configuration before performing any software update. See the module's *Management and Configuration Guide* (5991-8626) for instructions and more information.

ProCurve Networking periodically provides software updates through the ProCurve Networking Web site www.hp.com/go/procurve/software. After you acquire the new software file, use TFTP or FTP from the Web browser interface or the CLI to update the module software. See the module's *Management and Configuration Guide* (5991-8626) for instructions and more information.

Note

Downloading new software does not change the current module configuration. The module configuration is contained in a separate file that can also be transferred, for example, for archive purposes or to be used in another module of the same model.

Saving Configurations

The module operates with two configuration files:

Running-Config File: Exists in volatile memory and controls module operation. Rebooting the module erases the current running-config file and replaces it with an exact copy of the current startup-config file. To save a configuration change, you must save the current configuration in the running-config file to the startup-config file.

Startup-Config File: Exists in flash (non-volatile) memory and preserves the most recently-saved configuration as the “permanent” configuration. When the module reboots for any reason, an exact copy of the current startup-config file becomes the new running-config file in volatile memory.

In the **wireless-services** context of the CLI, you may use the **write memory** command to save changes made to the running-config file to the startup-up config file. Also, the system prompts you to save any unsaved changes when you leave the **wireless-services** context.

Saving the Current Configuration as the Start-Up Configuration

When you use the CLI to make a configuration change, the module places the change in the running-config file. If you want to preserve the change across reboots, you must save the change to the startup-config file. Otherwise, the next time the module reboots, the change will be lost.

To save configuration changes while using the CLI:

1. From the **wireless-services** context:

```
ProCurve Switch 5406zl(wireless-services-B)#write memory
[OK]
ProCurve Switch 5406zl(wireless-services-B)#
```

2. Verify that the **[OK]** message displays, indicating that the configuration was saved successfully. The current configuration is now saved as the startup configuration file, and the module will execute the file at each power-up.

See the module's *Management and Configuration Guide* (5991-8626) for more information on managing module configuration files.

ProCurve Software Code Designations

Software Letter	ProCurve Networking Products
C	1600M, 2400M, 2424M, 4000M, and 8000M
CY	Switch 8100fl Series (8108fl and 8116fl)
E	Switch 5300xl Series (5304xl, 5308xl, 5348xl, and 5372xl)
F	Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324
G	Switch 4100gl Series (4104gl, 4108gl, and 4148gl)
H	Switch 2600 Series, Switch 2600-PWR Series: H.07.81 and earlier, or H.08.55 and greater, Switch 2600-8-PWR requires H.08.80 or greater. Switch 6108: H.07.xx and earlier
I	Switch 2800 Series (2824 and 2848)
J	J.xx.xx.biz Secure Router 7000dl Series (7102dl and 7203dl)
J	J.xx.xx.swi Switch 2520G Series (2520G-8-PoE, 2520G-24-PoE)
K	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, 5400zl Series (5406zl, 5406zl-48G, 5412zl, 5412zl-96G), Switch 8212zl and Switch 6600 Series (6600-24G, 6600-24G-4XG, 6600-24XG).
L	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
M	Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 through M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 through M.08.95, or M.08.99 to M.08.100 and greater.
N	Switch 2810 Series (2810-24G and 2810-48G)
P	Switch 1810G (1810G-8, 1810G-24)
PA/PB	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
Q	Switch 2510 Series (2510-24)
R	Switch 2610 Series (2610-24, 2610-24/12PWR, 2610-24-PWR, 2610-48 and 2610-48-PWR)
S	Switch 2520 Series (2520-8-PoE, 2520-24-PoE)
T	Switch 2900 Series (2900-24G and 2900-48G)
U	Switch 2510-48
W	Switch 2910al Series (2910al-24G, 2910al-24G-PoE+, 2910al-48G, and 2910al-48G-PoE+)
VA/VB	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
WA	ProCurve Access Point 530
WM	ProCurve Access Point 10ag
WS	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
WT	ProCurve Wireless Edge Services zl Module and the ProCurve Redundant Wireless Services zl Module
Y	Switch 2510G Series (2510G-24 and 2510G-48)
Z	ProCurve 6120G/XG and 6120XG Blade Switches
numeric	Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.)

Support Notes and Clarifications

Release WT.01.03

WT.01.03 is the first software version for Wireless Edge Services zl Modules. ProCurve switches that support this module (Switch 5400zl Series and Switch 8212zl) require software version K.12.43 (or later).

The *Management and Configuration Guide* (5991-8626) includes detailed information on the features in software release WT.01.03. To download this guide, see [“Downloading Software and Documentation from the Web” on page 1](#).

This section contains information on the following:

[“Accessing the Web Browser Interface — In Case of Difficulty”](#)

[“Configuring Authentication for Web-Users”](#)

[“Special Characters for the ACL ID Field”](#)

[“Correction: SNMP v3 Default Password”](#)

[“Clarification: For Layer 3 Adoption, DHCP Server Option 189 Requires Value Type ‘String’”](#)

[“Correction: Stations per Module in a Layer 3 Mobility Domain”](#)

[“Correction: Disabling TKIP Countermeasures”](#)

[“Clarification: Setting Intrusion Detection with TKIP Countermeasures”](#)

Accessing the Web Browser Interface — In Case of Difficulty

Your Web browser or Java cache may trigger problems with initial access to your module. If you have difficulty with access to the Wireless Edge Services zl Module's Web management interface, you may need to complete these steps:

1. Clear your browser's cache.
2. Clear the Java cache.
3. Close the browser and re-open it.

The following instructions explain how to complete the first two steps. It is assumed that you have already updated the module's software and reset the module.

Clear the Internet Explorer (IE) Browser Cache

The following steps detail the process of clearing the cache in IE version 6. If you are using a different version, your steps might vary slightly.

Follow these steps to clear the cache:

1. Open IE.

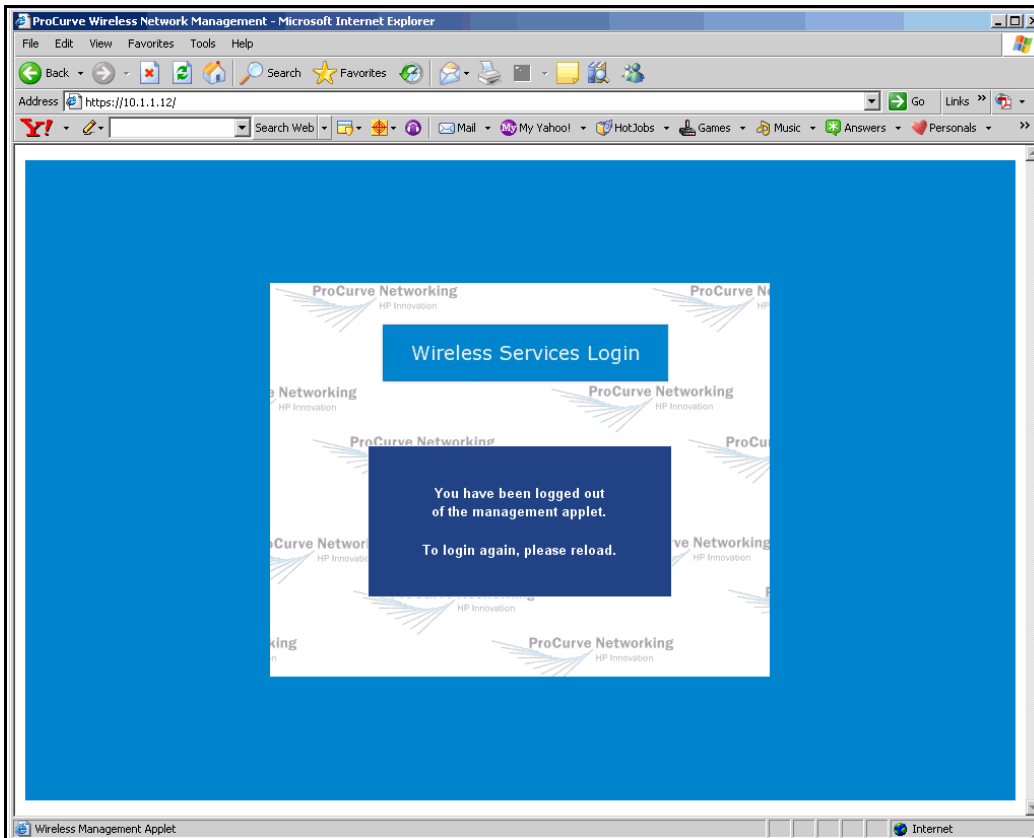


Figure 1. IE Browser

2. Select **Tools > Internet Options**. The **Internet Options** window is displayed.

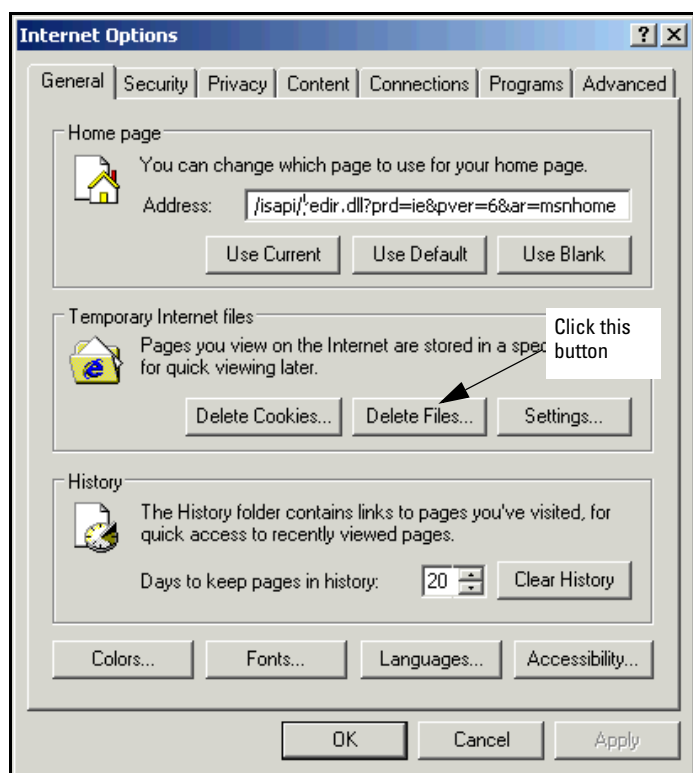


Figure 2. Tools > Internet Options

3. Make sure that you are in the **General** tab.
4. In the **Temporary Internet files** section, click **Delete Files**. The **Delete Files** window is displayed.

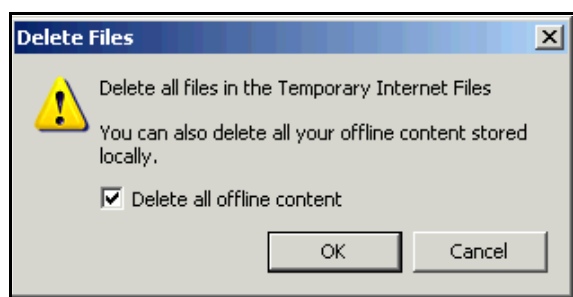


Figure 3. Delete Files

5. Check the **Delete all offline content** box.
6. Click the **OK** button.
7. In the **Internet Options** window, click the **OK** button.

Clear the Java Cache

The following steps explain how to delete the cache for Sun Java version 1.5 or higher on a Windows XP machine. The steps vary depending on whether your Java version is above or below. See either:

[“Clear the Cache for Sun Java Versions 1.5 and Higher” on page 7](#)

[“Clear the Cache for Sun Java Versions Prior to 1.5” on page 9](#)

Clear the Cache for Sun Java Versions 1.5 and Higher. Follow these steps to delete the Java cache:

1. Select **Start > Settings > Control Panel**.

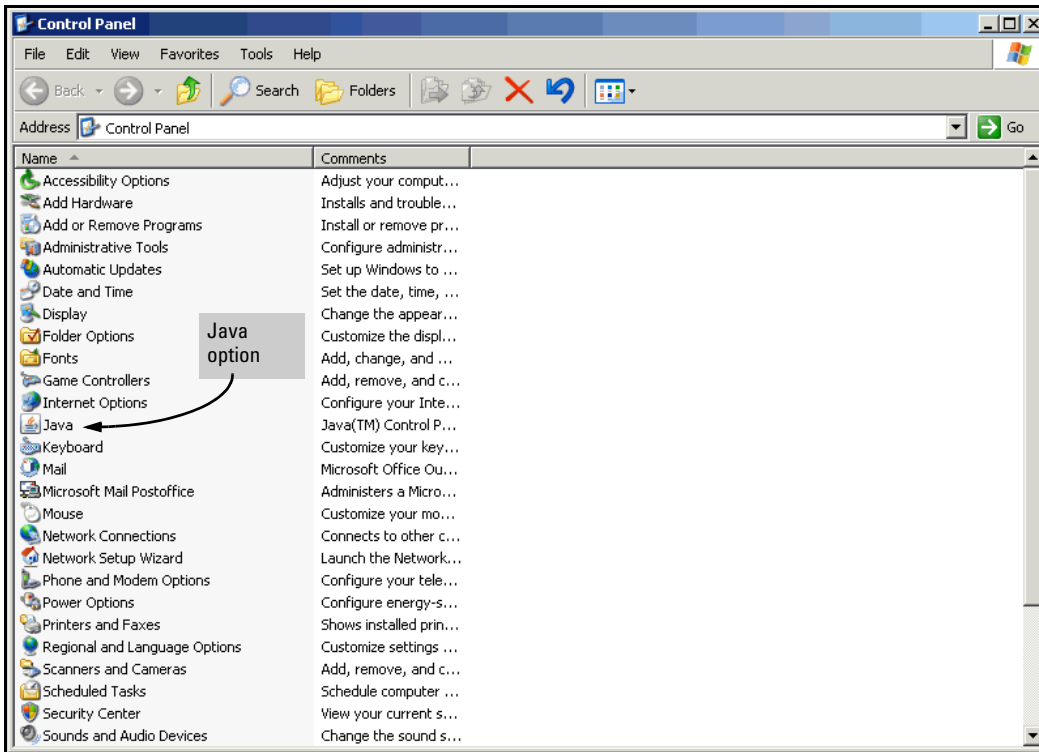


Figure 4. Control Panel

2. Select **Java**. The **Java Control Panel** window is displayed.

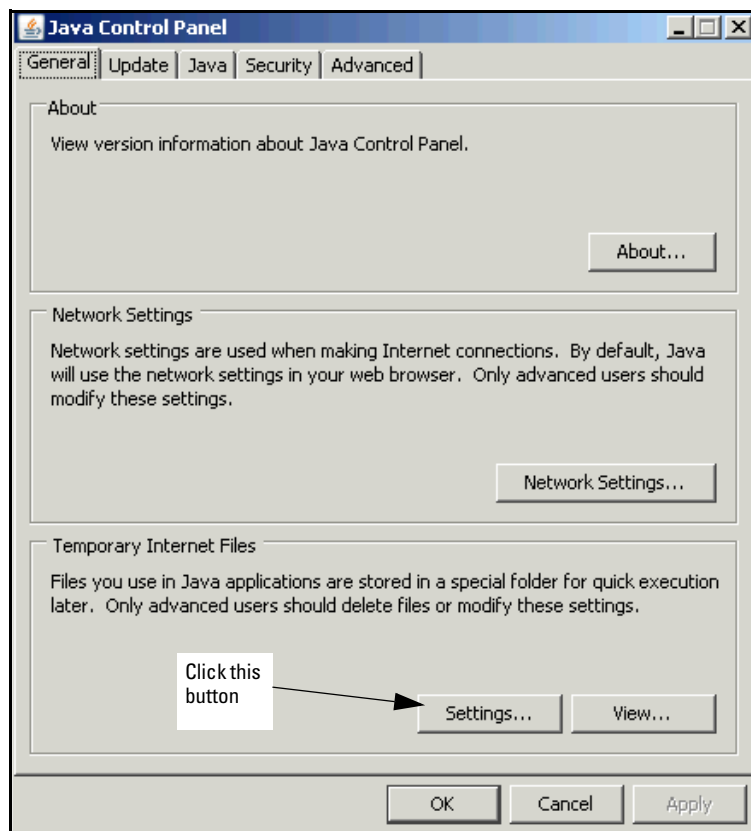


Figure 5. Java Control Panel

3. In the **Temporary Internet Files** section, click the **Settings** button. The **Temporary Files Settings** window is displayed.

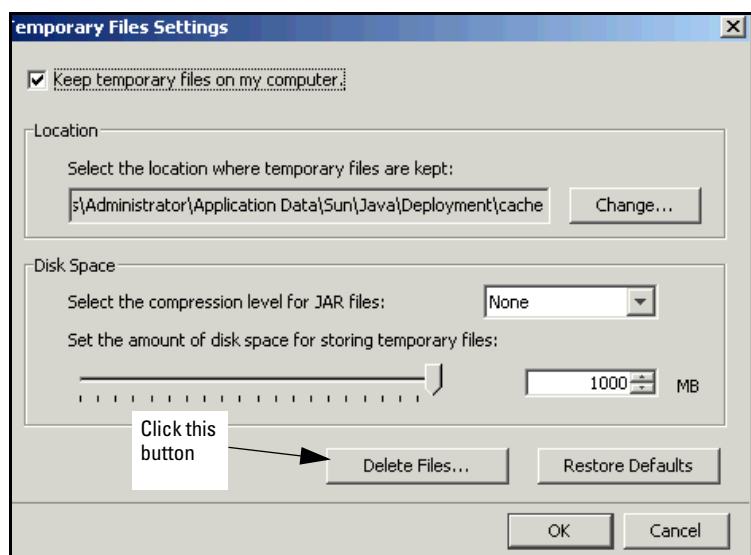


Figure 6. Temporary Files Settings (Java Control Panel)

- Click the **Delete Files** button. The **Delete Temporary Files** window is displayed.

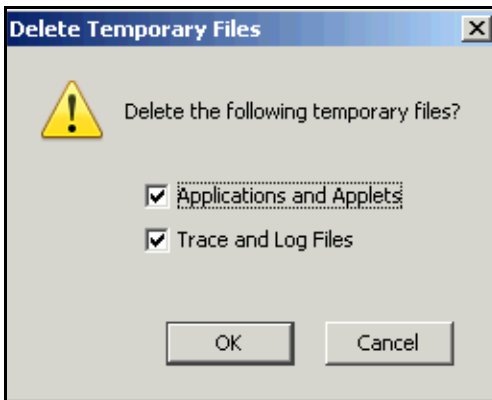


Figure 7. Delete Temporary Files (Java Control Panel)

- Make sure that the **Applications and Applets** box is checked.
- Click the **OK** button.
- In the **Temporary Files Settings** window, click the **OK** button.
- In the **Java Control Panel** window, click the **OK** button.

Clear the Cache for Sun Java Versions Prior to 1.5. Follow these steps to delete the Java cache:

- Select **Start > Settings > Control Panel**.

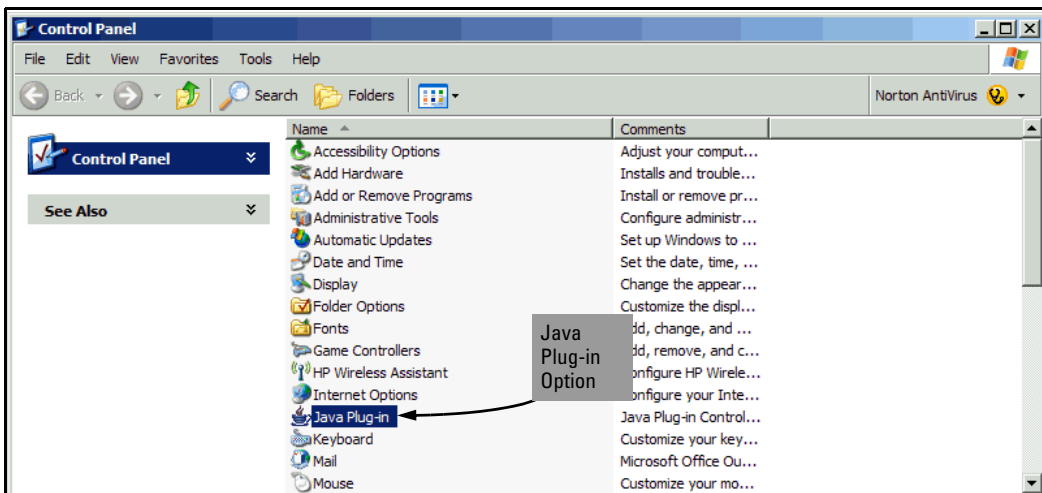


Figure 8. Control Panel

- Select **Java Plug-in**. The **Java Plug-in Control Panel** window is displayed.

Note

If your workstation has more than one Java applet, the Control Panel will display multiple Java Plug-in options. Complete the following steps for each to ensure that the correct cache is cleared.

3. Select the **Cache** tab.

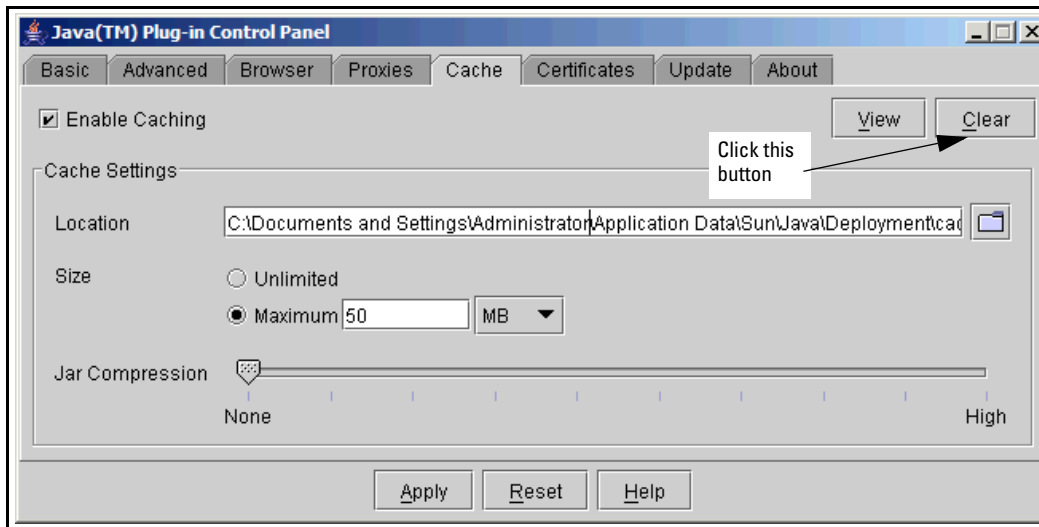


Figure 9. Java Plug-in Control Panel

4. You are prompted to confirm clearing the cache. Click the **Yes** button.

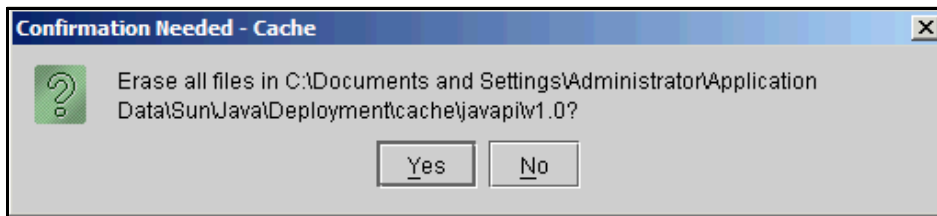


Figure 10. Java Plug-in Confirmation Needed Screen

5. Click the **Apply** button; then close the screen.

Restart the Browser

You are now ready to access the Wireless Edge Services zl Module's Web browser interface:

1. Close and re-open your browser.
2. Enter the IP address (or hostname) of your Wireless Edge Services zl Module in the browser.

3. The Java applet should begin to download from the module. You might need to activate the applet (as shown in Figure 11). Press **[Space]** or **[Enter]**.



Figure 11. Activate the Java Applet

4. After about a minute, the **Login** screen is displayed.



Figure 12. Login Screen for Wireless Edge Services zl Module

Configuring Authentication for Web-Users

Note Use this section to supplement the information in the chapter “Configuring the ProCurve Wireless Edge Services zl Module” in the *Management and Configuration Guide* (5991-8626).

Instead of (or in addition to) using the local list to authenticate users, you can use a RADIUS server. If the RADIUS server authenticates a user, that user has the rights configured on the RADIUS database.

Make sure that the configuration on the RADIUS server meets these requirements:

The user’s password is at least 8 characters.

SNMP v3 requires a password of at least this length. Your RADIUS server, however, may or may not enforce such a requirement. (For example, the Wireless Edge Services zl Module’s internal server does *not*.) Check the accounts for users that need management access to the module and, if necessary, set a new password of the correct length.

The RADIUS server supports vendor specific attributes (VSAs).

For the RADIUS server to properly authorize the management user, you must set two VSAs in the policy that the RADIUS server uses to authenticate the user. [Table 13](#) shows the proper values for the “HP-Management-Protocol” and the “HP-Management-Role” attributes.

Table 13. VSAs for Authorizing Management Users

Attribute	Type	Length	Vendor ID	Vendor Type	Vendor Length	Format	Vendor Value Decimal Format
HP-Management-Protocol	26	12	11 (HP)	4 (HP-Management-Protocol)	6	Decimal	5 = HTTP 6 = HTTPS
HP-Management-Role	26	12	11	1 (HP-Management-Role)	6	Decimal	1 = SuperUser 2 = Monitor 16 = HelpDesk Manager 17 = Network Administrator 18 = System Administrator 19 = WebUser Administrator

If the server does not send the proper VSAs, the user receives the monitor role (read-only) to the Web browser interface.

The module’s internal server does not support VSAs, so you should use the local server only to authenticate users that require read-only access.

Note

If you do not correctly configure the RADIUS server, you can lock yourself out of the Wireless Edge Services zl Module Web browser interface.

To fix the problem, access the module CLI through the wireless services-enabled switch. Enter this global configuration mode command to have the module authenticate Web-Users against its local list:

Syntax: aaa authentication login default local

Then configure at least one user in the local list:

Syntax: username <username> password <password>

The password must be between 8 and 32 characters.

Then assign the user rights sufficient to correct the problem. For example:

Syntax: username <username> privilege superuser

Special Characters for the ACL ID Field

As indicated in the chapter “Access Control Lists (ACLs)” of the *Management and Configuration Guide* (5991-8626), string names for ACL IDs may contain alphanumeric characters, but spaces and non-alphanumeric characters are not allowed. However, the following special characters may be used:

` ~ ! @ # \$ % ^ & * () _ - { } [] | : ; ' < > , .

Correction: SNMP v3 Default Password

The chapter “Configuring the ProCurve Wireless Edge Services zl Module” of the *Management and Configuration Guide* (5991-8626) incorrectly states that for the snmptrap user, the default password is “procurve”. Instead, the default password is “trapuser.”

Clarification: For Layer 3 Adoption, DHCP Server Option 189 Requires Value Type ‘String’

You must properly set up your DHCP server to support Layer 3 adoption of Radio Ports. Refer to your DHCP server documentation for instructions on adding private options and the configurations that your Radio Ports will receive.

For adopting Radio Ports at Layer 3, you must set up the DHCP option so that its code is **189**, and its value type is **string** (instead of Byte or IP).

Refer to the zl Module’s *Management and Configuration Guide* for more information.

Correction: Stations per Module in a Layer 3 Mobility Domain

The zl Module’s *Management and Configuration Guide* (February 2008), page 1-85, incorrectly states that a Layer 3 Mobility Domain can include up to 12 modules, each of which can support up to 500 stations. Instead, the number of local stations per module is 4096.

Correction: Disabling TKIP Countermeasures

TKIP countermeasures are used to prevent “man-in-the-middle” TKIP attacks by disabling client connections for a short period of time. In some cases, you may want to disable TKIP Countermeasures. The zl Module’s *Management and Configuration Guide* (February 2008) includes a command that is *not* available for disabling TKIP Countermeasures:

no support wireless tkip-countermeasures

The following command effectively disables TKIP Countermeasures:

```
ProCurve(wireless-services-C)(config-wireless)#wlan 1 dot11i tkip-cntrmeas-hold-time ?  
<0-65535> The hold-time in seconds. Default = 60
```

```
ProCurve(wireless-services-C)(config-wireless)#wlan 1 dot11i tkip-cntrmeas-hold-time 0
```

where **1** specifies the WLAN index in this example, and **0** specifies the hold-time (in seconds) in which clients are disconnected.

Clarification: Setting Intrusion Detection with TKIP Countermeasures

Intrusion Detection System (IDS) commands can be used to filter a station that set off IDS. Setting the following ids parameters will blacklist the client for the amount of time set in the ageout (ageout time can be up to one day).

```
ProCurve(wireless-services-C)(config-wireless)#ids anomaly-detection tkip-countermeasures enable
```

```
ProCurve(wireless-services-C)(config-wireless)#ids anomaly-detection tkip-countermeasures filter-ageout 60
```

where **60** in this example is the ageout duration (seconds) in which mobile units will be filtered out. A value of 0 - 86400 seconds can be configured.

Release WT.01.13

Release WT.01.13 is a *special* release for WESM zl modules purchased prior to April 1, 2008, in the European Union and selected countries/regions.

Regulatory restriction removal: this change allows customers in the European Union and selected countries/regions (including South Africa, Turkey, Morocco, and Croatia) who purchased their modules prior to April 1, 2008 to benefit from the software fixes and ProCurve MM 2.0 Automatic Update 1 (AU1) support introduced after WT.01.03, but without the new restriction in 802.11a channel availability released in WT.01.10.

Output from the command, **show ip dhcp binding** displays only the dynamic IP address bindings. To display the manually-configured DHCP bindings, use the following command:

```
show ip dhcp binding manual.
```

Release WT.01.15

Release WT.01.15 is a general release that may be used with WESM zl modules purchased prior to, or after, April 1, 2008, in the European Union and selected countries/regions, with channel restrictions as described below.

Regulatory restriction re-imposed as in WT.01.10: In the European Union and selected countries/regions (including South Africa, Turkey, Morocco, and Croatia), ProCurve Wireless Edge Services Modules, Access Points and Radio Ports purchased after April 1, 2008, are subject to new radar interference requirements that limit the available channels in the 5 GHz band. To comply with these new requirements, the operating channels impacted by this change have been removed. The available 5 GHz channels are now 36, 40, 44 and 48 (5.150 - 5.250 GHz).

Release WT.01.28

Logging Aggregation Time

The operation of the Logging Aggregation Time parameter as described in the *Management and Configuration Guide* and the Web interface *Help* require clarification.

Any message is immediately printed, unless it is identical to the previous one. If it is identical, then a counter is incremented instead. If a different message arrives, then the accumulated count is printed (%MGMT-4-V12AUTHERROR: Last message repeated x times), followed by the new message. If no new message arrives within the “Logging Aggregation Time” of the last duplicate, then the accumulated count is printed and the count is cleared.

Wireless Station Intrusion Detection Configuration

In Chapter 12 of the *Management and Configuration Guide*, the section “Configuring Thresholds for Station Intrusion Detection” does not clearly specify when a violation is logged. In addition, the Web Interface *Help* may incorrectly specify that a threshold must be exceeded to log a violation.

Violation Parameters: Station

Set the wireless station threshold value for each violation type. *If exceeded*, the wireless station will be filtered and displayed within the Filtered wireless stations screen.

Note: Setting a violation parameter to 0 will disable the option.

Violation Parameters: Radio

Set the radio threshold value for each violation type. *If met*, the violation will be logged.

Note: Setting a violation parameter to 0 will disable the option.

Violation Parameters: Wireless Module

Set the wireless Module's threshold value for each violation type. *If met*, the violation will be logged.

Note: Setting a violation parameter to 0 will disable the option.

Enhancements

Unless otherwise noted, each new release includes the enhancements added in all previous releases. To review the enhancements associated with the most recent general release, see [“Release WT.01.17 Enhancements” on page 17](#).

Release WT.01.03 Enhancements

WT.01.03 is the first software version for Wireless Edge Services zl Modules.

Note The *Management and Configuration Guide* (5991-8626) provides detailed information on the features in software release WT.01.03. Download this guide for more information. To download this guide, see [“Downloading Software and Documentation from the Web” on page 1](#).

Features

The following features are available with release WT.01.03 software. For more information, see the *Management and Configuration Guide* (5991-8626) released with WT.01.03 (or later) software.

Table 14. Key Features in Version WT.01.03 Software

Feature	Description
Layer 3 RP adoption	Adopt Radio Ports (RPs) that are installed on a different subnetwork
Internal RADIUS server	Authenticate users with an internal (built-in) RADIUS server.
Firewall	Filter routed traffic through an internal firewall.
IP and MAC ACLs	Control traffic to and from wireless stations through Access Control Lists (ACLs) based on IP and MAC addresses.
Network Address Translation (NAT)	Provide Network Address Translation (NAT) services for traffic routed between two subnetworks, typically between the wireless and wired network.
Internal DHCP server	Provide DHCP services for wireless clients on a VLAN.
Fast Layer 2 roaming between modules	Wireless stations can disassociate with one Radio Port, and quickly reassociate with a different Radio Port under the control of the same module.
Layer 3 mobility	Wireless stations can disassociate with one Radio Port, and quickly reassociate with a different Radio Port under the control of different modules in the same Layer 3 mobility domain.
sFlow support	A module's sFlow agent monitors each radio and samples wireless traffic for an sFlow collector.
Secure NTP	Configure the module to take its time from an Network Time Protocol (NTP) server, or act as a secure NTP server for other devices.
Web-Users accounts	Create accounts for Web-Users, allow various levels of access to the module's Web browser interface.
ProCurve Identity Driven Manager (IDM) QoS	Supports Quality of Service (QoS) settings created through IDM.

Capabilities

Capabilities and scalability of the ProCurve zl Wireless Edge Services Module are summarized in the following table.

Note Unlike Wireless Edge Services xl Modules (for Series 5300 xl switches), zl Modules running software version WT.01.03 (or later) do not support GRE Tunnels.

Table 15. Summary of Capabilities and Scalability in WT.01.03

Feature/Function	WT.01.03
Throughput - Unencrypted	2000 mbits
Maximum number of Radio Ports supported	156
Maximum number of associated stations	4096
Maximum number stations per radio	256
Maximum number of modules in Redundancy Group	12
Maximum number of VLANs per module	32
Radio Port Failover time (Layer 2)	20 sec typical
Maximum number of static routes	300
Maximum number RADIUS Authentications per second	4 Internal / 3 LDAP
Maximum number of DHCP Lease Grants per second	15
Maximum number of modules in Layer 3 Roaming Group	12

Release WT.01.13 Enhancements

Support for Client Location Confidence in ProCurve Mobility Manager

To support the client location confidence feature in ProCurve Mobility Manager 2.0 Automatic Update 1 (AU1), the logging of client probe requests (a “Probe List”) can be enabled through the switch’s Command Line Interface (CLI).

To enable logging of client probe requests, use the **station probe-history enable** command from the wireless configuration context. For example:

ProCurve<wireless-services-A><config-wireless># station probe-history enable

where the WESM zl is installed in slot A of the switch in this example.

Release WT.01.17 Enhancements

Enhancement (PR_0000000844) — Added functionality on the module to enable Web-authentication redirection to use a DNS name rather than an IP address.

Release WT.01.20 Enhancements

VLAN (PR_0000002129) — Increased VLAN limit to 64 (from 16) for Uplink/Downlink ports.

Software Fixes

Unless otherwise noted, each new release includes the software fixes added in all previous releases. To review the software fixes associated with the most recent general release, see [“Release WT.01.16” on page 19](#).

Release WT.01.03

Release WT.01.03 was the first software release for the ProCurve Wireless Edge Services zl Module.

Release WT.01.10

Release WT.01.10 was released to Manufacturing only, and is not a general release.

Problems resolved in Release WT.01.10

Infrastructure (39309) — Even when the redundancy heartbeat-period has been configured to a non-default value and that configuration change has been saved, the module reverts to the default value of 5 seconds following a reload.

Infrastructure (45510) — Incoming packet counters are not incrementing properly for VLAN and ACL interfaces.

Infrastructure (45577) — The Web management interface does not provide the ability to configure the local RADIUS server's IP address.

Radio Port/Wireless (46298) — An incorrect DNS string was pushed to the radio ports when they are first adopted by a module on a software version capable of layer 3 adoption.

Security (45549) — The allowed configuration value range for the RADIUS client shared secret was not consistent between the CLI and Web management interface. This fix removes the 4 character minimum from the Web management interface.

Wireless (45552) — Pairwise Master Key (PMK) caching allows the module to store a station's PMK after the station disassociates with a Radio Port so that the key remains in place if the station re-associates with a different Radio Port. Prior to this fix, network administrators had to disable PMK caching to use the ACL features in IDM. This fix will ensure that IDM ACLs will remain in place after a roam, with PMK caching enabled.

Wireless (46457 and 46292) — In the European Union and selected countries/regions (including South Africa, Turkey, Morocco, and Croatia), ProCurve Wireless Edge Services Modules, Access Points and Radio Ports purchased after April 1, 2008, are subject to new radar interference requirements that limit the available channels in the 5 GHz band. To comply with these new requirements, the operating channels impacted by this change have been removed. The available 5 GHz channels are now 36, 40, 44 and 48 (5.150 - 5.250 GHz).

Release WT.01.13

Release WT.01.13 is a *special* release for WESM zl modules purchased prior to April 1, 2008, in the European Union and selected countries/regions.

Problems resolved in Release WT.01.13

Wireless (46295) — *Regulatory restriction removal*; this change allows customers in the European Union and selected countries/regions (including South Africa, Turkey, Morocco, and Croatia) who purchased their modules prior to April 1, 2008 to benefit from the software fixes and ProCurve MM 2.0 Automatic Update 1 (AU1) support introduced after WT.01.03 without the new restriction in 802.11a channel availability.

Wireless (46290) — The station probe table was added for support of ProCurve MM 2.0 Automatic Update 1 (AU1) and its Location Confidence feature. For more information, see [“Release WT.01.13 Enhancements” on page 17](#).

Release WT.01.14

Release WT.01.14 was not a general release.

Release WT.01.15

Release WT.01.15 was a general release.

Problems resolved in Release WT.01.15

Wireless (00677) — An incorrect RSSI value is displayed in response to an SNMP walk.

Wireless (00681) — All the wireless stations in the Probe list inaccurately report the same RSSI.

Wireless (01085) — CPU utilization in the module may approach 100% the day following application of ProCurve's Mobility Manager 2.0 Automatic Update 1 (AU1) release.

Wireless (14986) — A faulty radio port may trigger repeated reboots due to the module experiencing ccserver crashes. This fix prevents the module from adopting faulty radio ports.

Wireless (46457, 46292, 46295) — Release WT.01.15 may be used with WESM zl modules purchased prior to, or after, April 1, 2008, in the European Union and selected countries/regions with channel restrictions as described below.

Regulatory restriction re-imposed as in WT.01.10: In the European Union and selected countries/regions (including South Africa, Turkey, Morocco, and Croatia), ProCurve Wireless Edge Services Modules, Access Points and Radio Ports purchased after April 1, 2008, are subject to new radar interference requirements that limit the available channels in the 5 GHz band. To comply with these new requirements, the operating channels impacted by this change have been removed. The available 5 GHz channels are now 36, 40, 44 and 48 (5.150 - 5.250 GHz).

Release WT.01.16

Release WT.01.16 was not a general release.

Problems resolved in Release WT.01.16

Infrastructure (PR_0000002266) — Configuration file may fail to load properly onto the redundant module from the update server.

Security (PR_0000002283) — When using Web Authentication, a Guest group member with valid credentials may not be allowed access to the network.

Applet (PR_0000002282) — When using the Web management interface to enter a domain name in the **Network Services > Internet Protocol > Global Settings** tab, the change will not be displayed on the CLI and will not be saved.

Infrastructure (PR_0000002284) — When using the CLI to reset all RPs adopted by a module, an idmagent core file is generated in error. The module continues to work normally after the core file is generated.

ESPD (PR_0000004548) — When PMK caching is enabled, and a client using WPA/WPA2 disconnects and ages out of the table, log messages like the following may be seen (date, time, severity, and IP address stamps removed for clarity).

```
espd: ESPd_emi_req() - Invalid OpCode
```

Security (PR_0000000752, PR_0000002283) — When creating a guest account on the module with local Radius and Web authentication, the start time for the guest account will be 2 hours earlier than the actual local time, which results in a Web authentication failure.

Release WT.01.17

Release WT.01.17 was not a general release.

Release WT.01.18

Release WT.01.18 was not a general release.

Problems resolved in Release WT.01.18

Wireless (PR_0000004757) — Wireless clients stop getting an IP address from the DHCP server after an extended period of time.

Wireless (PR_0000004761) — RPs transmitting bad radio types will cause WESM(s) to reboot.

Infrastructure (PR_0000003687) — Module periodically loses configuration visually through the CLI, but continues to operate normally until a reboot, which causes the configuration to be lost.

Wireless (PR_0000004763) — Wireless clients may be unable to roam between modules within the same SSID after being authenticated.

Release WT.01.19

Release WT.01.19 was not a general release.

Problems resolved in Release WT.01.19

Security (PR_0000003978) — Web-authenticated clients do not disconnect after user logs off.

Release WT.01.20

Release WT.01.20 was not a general release.

Problems resolved in Release WT.01.20

Web UI (PR_0000002041) — A Guest account created through the Web User Interface will not be saved after a reload of the WES module.

VLAN (PR_0000002129) — Increased VLAN limit to 64 (from 16) for Uplink/Downlink ports.

If VLANs are tagged to uplink or downlink ports, the WESM will only recognize the first 64 VLANs tagged (in ascendant order, i.e. VLAN 10, VLAN 20, etc.) and transfer traffic (layer 2, layer 3 only for the ones that are interfaces and configured in the WESM on the Ethernet tab below Network Setup) between the WESM and the chassis. For VLAN numbers 65 and higher the WESM will not be able to transfer the traffic and stations that are in a VLAN in the 65+ range will not be able to communicate correctly. There is a total of 64 uplink tagged VLANs and 64 downlink tagged VLANs, for a combined total of 128 VLANs.

Web UI (PR_0000003233) — On the Web User Interface, updated Help information regarding the Web Access Control features.

Web UI (PR_0000003782) — Unable to add a radio with number greater than 1000 as an index through the Web User Interface.

Web Authentication (PR_0000003811) — Web authentication redirection uses hostname and not the FQDN (hostname.domainname) resulting in certificate warnings.

Web UI (PR_0000003935) — On the Web User Interface, updated Help information for MAC Authentication features.

CLI (PR_0000005515) — DHCP client becomes disabled when configuring interface through the CLI.

Redundant module (PR_0000005593) — Redundant module defaults to active mode after restoring factory defaults.

Web UI (PR_0000005723) — On the Web User Interface, updated Help information for Web Authentication features.

Radio (PR_0000006089) — Increased character limit in the radio description field to 32.

WMM (PR_0000006215) — WES module resets when using WMM with dhcp-sniff enabled.

CLI (PR_0000006367) — Using the CLI to configure the 'hostname' and/or 'snmp-server sysname' results in different data field restrictions.

Web UI (PR_0000006378) — Shared Secret password display is not encrypted under the Web Users page.

CLI (PR_0000007410) — Domain name error is displayed when generating a CSR via CLI.

Web Authentication (PR_0000007696) — Web authentication credentials not being cleared after session timeout.

Web UI (PR_0000009408) — The Guest Registration login page is delayed 5 minutes from the module time causing login failure.

Web Authentication (PR_0000009647) — Increased the maximum number of stunnel client instances.

SVP (PR_0000011398) — Corrected unacceptable Response Times for WPA / WPA2 security negotiation.

Authentication (PR_0000012073) — Multicast packet filter limited broadcasts impacting connectivity for Windows Vista DHCP clients.

Web Authentication (PR_0000013397) — If the Domain Name is left blank, a null text string will be entered when creating a Web authentication redirect URL.

LDAP (PR_0000014089) — LDAP user string mis-interprets special characters.

Hang (PR_0000015675) — Appearance of random WESM hangs. No traffic being passed and no access to CLI or Web UI.

SNMP (PR_0000015676) — SNMPd memory usage exceeds maximum threshold and SNMPd process is restarted by process monitor.

Release WT.01.21

Release WT.01.21 was not a general release.

Problems resolved in Release WT.01.21

DHCP (PR_0000006234) — When selecting the 'Use DHCP to obtain IP Address automatically' option, the IP Address field does not become grayed out.

Web UI (PR_0000015632) — Display performance improvements made to the Web UI.

Release WT.01.22

Release WT.01.22 was not a general release.

Problems resolved in Release WT.01.22

MAC Authentication (PR_0000004541) — MAC authentication fails when using multi-colon format as MAC Address format.

Reboot (PR_0000012106) — Module would hang and/or reboot with high CPU and RAM usage.

Web Authentication (PR_0000015682) — Reset limit for multiple Web authentication redirects during authentication process.

Release WT.01.23

Release WT.01.23 was not a general release.

Problems resolved in Release WT.01.23

DHCP (PR_0000004557) — Using the Web UI to edit DHCP IP Ranges will not be saved.

Web UI (PR_0000009232) — Guest accounts created through the Web UI would fail authentication, but work correctly when created through the CLI.

Web UI (PR_0000009999) — WES module resets configuration file back to default values when editing configuration file through the Web UI.

Web UI (PR_0000015784) — Using the Web UI to configure a guest account with Time zone Etc/GMT-12 from the Local RADIUS Server, the guest account will not be saved.

Release WT.01.24

Release WT.01.24 was not a general release.

Problems resolved in Release WT.01.24

Web UI (PR_0000017373) — User is unable to install the module license through Web UI.

Release WT.01.25

Release WT.01.25 was not a general release.

Problems resolved in Release WT.01.25

Reboot (PR_0000014489) — WES module reboots sometimes if RAM usage is extremely high.

Reboot (PR_0000016358) — WES module may freeze or reboot with high CPU utilization.

Release WT.01.26

Release WT.01.26 was not a general release.

Problems resolved in Release WT.01.26

DHCP (PR_0000000757) — RP adoption using DHCP does not work when DHCP server is configured with Option 43 and Option 189.

Neighbor AP (PR_0000000866) — Incorrect RSSI values captured from Neighbor AP detection.

ACL (PR_0000002513) — Identity Driven Manager ACLs fail to apply when multiple ports are assigned in an ACE.

Web UI (PR_0000005510) — The System Maintenance Software filter does not work with two dates filters in the drop down menu, Built Time and Install Time.

Statistics (PR_0000005519) — When opening several graphs on the Statistic tab, the graphs overlaps the statistical information.

Alert (PR_0000006294) — WES primary module intermittently reports the redundant module as unreachable.

Configuration (PR_0000008352) — Updated error message in pop up window when trying to copy into running configuration.

Web Authentication (PR_0000015015) — Deleting domain name for Web Authentication redirect does not take effect until WES module is rebooted.

Reboot (PR_0000015169) — WES module would reboot when packet buffer size threshold was exceeded.

Web UI (PR_0000015181) — Using the Web UI to create a guest account, the font type displayed was hard to read whether the character was lower or upper case of certain characters.

Time zone (PR_0000016393) — Incorrect time zone offset displayed between the Web UI and the CLI.

Web UI (PR_0000016395) — Port, Retries and Timeout columns are not displayed on the Authentication Web page.

Web UI (PR_0000016733) — MAC Authentication configuration window will not close after hitting the "OK" button.

Reboot (PR_0000017532) — WES module spontaneously reboots 3 - 4 times per day.

ACL (PR_0000017548) — Identity Driven Manager ACLs fail to apply when multiple ports are assigned in an ACE.

WMM (PR_0000018211) — When editing WMM settings under WLAN Setup -> WMM page, the SSID name is not completely displayed.

RADIUS (PR_0000018213) — Unable to create a Shared Secret key of less than 4 characters in a Domain Proxy Server.

Web UI (PR_0000018223) — Sort by VLAN is not working properly in the Network Setup page.

Reboot (PR_0000018541) — While executing a tech dump, the WES module may intermittently reboot.

Web Authentication (PR_0000018543) — The redirection URL will display a double-domain name, if a hostname includes the domain name and Web authentication redirect to hostname is enabled.

Authentication (PR_0000019045) — Client login credentials remain after disconnecting.

Release WT.01.27

Release WT.01.27 was not a general release.

Problems resolved in Release WT.01.27

Web UI (PR_0000016304) — Shared Secret password is displayed as plain text when editing RADIUS Server parameters.

CLI (PR_0000038818) — CLI will hang or freeze when 40 or more ACEs are applied to authenticated users.

ACL (PR_0000019095) — When configuring ACLs in a RADIUS server, if an ACE has a range of ports with spaces around the hyphen, the server will fail to authenticate the user, even when the ACE is valid.

Web UI (PR_0000018220) — Within the **Network Setup > Ethernet** page, sorting VLANs by selecting the **IP Address** or **Subnet Mask** column headings does not work.

Upgrade (PR_0000017696) — After a software upgrade, the WESM displays an “upgrade has been completed” message, but does not indicate that a WESM reboot is required to complete the upgrade.

Release WT.01.28

Release WT.01.28 is a general release and includes software fixes for all prior releases.

Release WT.01.29

Release WT.01.29 was not a general release.

Problems resolved in Release WT.01.29

Web UI (PR_0000016366) — System Name had different restrictions when being set through the Web UI and CLI. The CLI required a letter as the first character and did not accept spaces in the System Name.

Web UI (PR_000018221) — Web UI displays different results from the CLI when the same SNMP Access Control is configured with two different community names.

CLI (PR_0000018295) — When using the same community name, the Web UI functioned correctly but the CLI would not allow the use of the same community name and displayed the error message: "%Error: Community string already in use".

Authentication (PR_0000040156) — Web User Authentication against an external RADIUS Server does not work when the '**Number of Retries to communicate with RADIUS Server**' value is set to 0.

CLI (PR_0000037878) — The '**edit**' command under the CLI does not function properly.

System Maintenance (PR_0000017549) — When a software image has been upgraded to the WESM and the WESM has not been reloaded, if a second image is upgraded or the upgrade process is aborted before completion, the WESM will not be accessible via Web UI or CLI.

Workaround: The WESM module must be removed from the switch chassis and then re-inserted into the chassis, or the switch must be power cycled.

SNMP (PR_0000017878) — Radio description could be incorrectly configured as blank via SNMP.

Web UI (PR_0000040129) — Unable to clear the IP address and subnet mask values from any interface when using the Web UI. The CLI functions correctly.

System (PR_0000041085) — Increased the allotted size of log message table.

Authentication (PR_0000001238) — The same RADIUS server IP address can be entered multiple times in the Radius server IP table.

Alarm Log (PR_0000040265) — When in the Alarm Log and attempting to display alarm details, the **Detail** button generates the following error message: "Failed to get the alarm details. Please retry".

CLI (PR_0000039943) — The CLI **#diff startup-config running-config** command does not display the difference between the configuration files.

Reports (PR_0000006376) — Column titles of the Network Statistics report does not match the labels in the Graphs and Detailed Information screens.

Web UI (PR_0000018380) — An incorrect row is reset after sorting the sFlow Receivers table and selecting the reset button.

System (PR_0000039264) — IDM Attributes are not displayed correctly by the WESM in Wireless Stations Information.

Authentication (PR_0000040149) — Key Name and Key Size fields are not grayed out when creating a new self signed certificate using the Certificates Wizard.

VLAN (PR_0000040271) — Cannot tag the uplink port of the WESM on more than 64 VLANs.

Web UI (PR_0000040566) — When using the Web UI to select and delete multiple rows of a table, only the first row is deleted.

Release WT.01.30

Release WT.01.30 was not a general release.

Problems resolved in Release WT.01.30

System (PR_0000044609) — After configuring an interface as the Management Interface, the interface will lose its IP address.

Web Authentication (PR_0000039635) — Users connected to an 802.1X authentication SSID will experience loss of connectivity, causing multiple sys-log messages indicating an "Invalid OpCode", eventually requiring a WESM reboot.

CLI (PR_0000042088) — CLI command, "**show wireless Radio Port**" displays incorrect VLAN ids for adopted Radio Ports.

System (PR_0000041083) — Reduced Broadcast Key Rotation intervals to a value of 5 minutes (300 seconds) to prevent WPA-enabled stations from losing connection.

Time (PR_0000039627) — Timezone GMT offsets are not correct.

Web UI (PR_0000005513) — When using the Web UI to connect to the WESM and changing the IP address of the management VLAN, an error message is displayed with incorrect information that the IP address is already assigned to another virtual interface.

System Maintenance (PR_0000012043) — Unable to transfer a configuration file to NVRAM or system directories unless the file already existed in these directories.

Web UI (PR_0000012157) — Secure NTP Status page always displays the Leap value as Synchronized, whether the Secure NTP feature was configured or not.

Web UI (PR_0000042557) — In the Device Information screen, a wireless station's detailed information is not refreshed after a parameter is changed.

CLI (PR_0000042699) — CLI command "**archive tar/table**" is not functioning properly; the WESM's CLI connection is closed and the prompt reverts to the switch's CLI.

CLI (PR_0000042700) — CLI command, "**archive tar/xtract**" is not functioning properly when the tar file is stored in the WESM's flash memory. The extracted Files directory is created but the files are not extracted.

Release WT.01.31

Release WT.01.31 was not a general release.

Problems resolved in Release WT.01.31

DHCP (PR_0000008356) — Internal DHCP Server does not provide IP addresses to wireless clients when a Host Pool is created in a Network Pool and the remaining Network Pool IP addresses have been excluded.

Radius (PR_0000041880) — WES module not allowing wireless clients to authenticate from the Secondary RADIUS Server (local) when the Primary RADIUS server is not available.

Syslog (PR_0000042414) — A time difference exists between the WES module's "real system time" and the timestamp of event logs.

Radius (PR_0000043966) — Local RADIUS Server stops running when including double quotes in the group name. For example, "Group".

Web UI (PR_0000042251) — When wireless client is running Mac OS X, the Web User Interface displays missing labels on action buttons or the Web interface not completely loading.

Radio Adoption (PR_0000017877) — An existing Radio configuration (Radio Index and Radio MAC address) can be overwritten via the CLI without receiving an error message.

VLAN (PR_0000044610) — An incorrect error message is displayed after configuring a VLAN as a Management Interface within the Network Setup screen.

IP Addressing (PR_0000044611) — An incorrect error message is displayed after configuring a static VLAN Interface IP address to use DHCP to obtain an IP address.

Release WT.01.32

Release WT.01.32 was not a general release.

Problems resolved in Release WT.01.32

File Handling (PR_0000012041) — When using the Web User Interface to transfer a large configuration file that exceeds the module's available flash storage space, an incorrect status message that the file transfer was successful is displayed, when in fact it is was not saved.

Encryption (PR_0000047389) — Editing an existing WEP 64 Pass key does not re-generate or become active after pressing the Enter key. An incorrect status OK message is displayed. Existing wireless clients remain connected due to the new Pass key not being generated and becoming active.

Encryption (PR_0000047390) — Editing an existing WEP 128 Pass key does not re-generate or become active after pressing the Enter key. An incorrect status OK message is displayed. Existing wireless clients remain connected due to the new Pass key not being generated and becoming active.

Web UI (PR_0000042652) — Configuring a friendly LLDP system name within Radio setup does not take effect after pressing the OK button. Viewing the LLDP Remote Device Information Details from the CLI incorrectly displays the Sys Name as a Hex number instead of the configured friendly LLDP system name.

Release WT.01.33

Release WT.01.33 is a general release.

Note

After upgrading software, your Web browser or Java cache may retain temporary data from the previous software version and may trigger problems with initial access to your module. We recommend clearing your Web browser and/or Java cache prior to accessing the Web management interface.

If you have difficulty with access or configuration on the Wireless Edge Services zl Module's Web management interface, see [“Accessing the Web Browser Interface — In Case of Difficulty” on page 4](#).

Problems resolved in Release WT.01.33

Radius (PR_0000044297) — WES module fails to transmit RADIUS Accounting On / Off messages to RADIUS servers after the WES module is shut down or restarted.

Authentication (PR_0000050245) — 802.1X credential changes are not applied to Radio Ports automatically until the Radio Port is rebooted.

Configuration (PR_0000003689) — If an existing WES module is replaced by a new WES module, the host Switch retains and applies expired module configurations to the replacement module instead of applying default values.

Web UI (PR_0000050746) — When using the Web User interface to view ACLs in the Security screen, the display is incorrectly limited to only 10 lines of the ACL.

Web UI (PR_0000046621) — Using the Web User Interface Filtering utility within the Radio Configuration screen to display a Radio Port list of 31 or more Radio Ports, the report will display incorrect information or no results at all.

Web UI (PR_0000018218) — Using the Web User Interface to view the Network Setup Internet Protocol screen, electing to sort by IP address does not function correctly.

Performance (PR_0000044687) — WES module occasionally reports high CPU utilization under certain conditions.

Performance (PR_0000047930) — WES module reporting sFlow and snmpd daemon log files consuming high CPU resources, requiring the module to be rebooted.

Performance (PR_0000049035) — WES module reporting sFlow daemon log files consuming high CPU resources, causing the module to crash.

Authentication (PR_0000054126) — Wireless clients cannot re-authenticate to WES module when using 802.1X. Clients frequently receive time-out and retry messages, causing the wireless network to become unstable.

Known Software Issues and Limitations

This section identifies known issues and limitations that you may encounter when using a ProCurve Wireless Edge Services zl Module (J9051A) or a ProCurve Redundant Wireless Services zl Module (J9052A). For the issues and limitations associated with the most recent general release, see [“Release WT.01.10” on page 33](#).

Note

When updating software from version WT.01.03 to any newer version, a module in a redundancy group may fail to rejoin the group if a non-default Heartbeat Period for the group is used. The software update will reset the Heartbeat Period to the factory-default value (5 seconds). To work around this issue, use one of the following methods:

- **Before updating the modules:** Before updating the software on the modules in a redundancy group, reset the redundancy group parameters to default values for all group modules.
- **After a module is updated:** After a software update, reconfigure the Heartbeat Period back to its pre-update value (to match the other redundancy group modules' Heartbeat Period setting).

For instructions and more information, see the module's *Management and Configuration Guide* (5991-8626) on the ProCurve Web site (www.hp.com/go/procurve/manuals).

Release WT.01.03

Release WT.01.03 is the first software release for the ProCurve Wireless Edge Services zl Module (J9051A) and the ProCurve Redundant Wireless Services zl Module (J9052A).

Applet (39709) — Regardless of whether a wireless client station is using the WMM power save feature, the Device Information -> Wireless Stations -> Details -> QoS information reports, "UAPSD enabled for: nothing". This display issue does not affect the function of the unscheduled automatic power save delivery (USPSD) feature.

Applet (41087) — There is an uninformative error message when the user tries to attach more than one ACL to a WLAN. The error message, "Unable to save - Wrong data type" should more accurately indicate that there is already an ACL attached to the interface.

Applet (41343) — After making a configuration change without applying the change, the Web management interface allows you to change Network Setup tabs from Configuration to Module Statistics without warning you that your changes will be lost.

Applet (41387) — The "wrong value" error triggered by configuration of overlapping excluded DHCP ranges is uninformative. The error should mention that overlapping IP address ranges are not permitted.

Applet (40023) — The Web management interface should disable (gray out) the **Delete** button when both the startup-config and running-config are chosen. Despite the presence of the delete option, running-config cannot be deleted; this is appropriate behavior.

Applet (40766) — The Web management interface allows removal of an ACL or ACE when it is in use by NAT.

Best Practice: Review the configuration and attachment of ACLs as part of the planning process prior to ACL deletion.

Applet (40950) — The list of ACLs displayed by the Web management interface is ordered arbitrarily (e.g. not ordered alphabetically, numerically, or by type). Be sure to check the entire list if you are having difficulty finding an ACL you have configured, scrolling to the bottom of the list if necessary.

Applet (41184) — The Web management interface Ethernet Configuration screen does not properly gray out all the appropriate fields; enabling DHCP grays out only the subnet mask, but not the IP fields. Additionally, though the mask is grayed out, the dots in the field are not grayed out. This does not have a functional consequence.

Applet (41215) — Since the ability to copy to the running-config has been removed from the Web management interface, the **system:** button should not be displayed on the Management -> System Maintenance - Config File -> Transfer -> browse for location popup window.

Workaround: Attempts at transferring to the file provide a meaningful message in the lower left window of the Web management interface.

Applet (41372) — After deleting a dynamic NAT entry and NAT interface from the Web management interface, the screen does not properly repaint the area where a popup dialog box was placed.

Applet (41423) — A static NAT entry is deleted if one of the parameters is modified using an invalid value.

Workaround: If you are having problems with static NAT entries being deleted immediately after using the Web management interface for configuration or modification, double check that all your configured parameters are valid and view the configuration file to confirm that the intended NAT rules are in place.

Applet (41504) — The Web management interface fails to warn the user if an ACE (Access Control Entry) that already exists is configured again. The ACE is appropriately disregarded rather than saved, but the user is not informed about why this action occurred.

Applet (41751) — In the Web management interface, the **Transfer Files** button is enabled even when there are no core or panic files present.

Applet (41761) — When inserting DHCP IP address ranges (Network Setup -> DHCP Server -> Configuration -> Add -> Included Ranges window of the Web management interface), use of the tab key cycles the cursor between the Start IP and End IP fields without progressing to other fields. The user will have to use the mouse to get to the other parameter fields.

Applet (41764) — The tab key does not allow the user to cycle through the various server fields of the Web management interface page for Network Setup -> DHCP Server -> Configuration -> Add -> Servers fields. The user will have to use the mouse to progress through the various parameter fields.

Applet (41992) — The Web management interface's Device Information page erroneously displays the Trouble-shooting -> Panic Snapshot page. The trigger for this event is unknown.

Applet (41768) — There is inconsistent behavior between CLI and Applet while configuring the preferred and alternate methods for user login. The Applet requires that both a preferred and alternate method be specified, but the CLI does not have any requirement for an alternate method.

Applet (38562) — The Web management interface allows the universal broadcast address (255.255.255.255) to be configured as a DNS IP address.

Applet (39807) — There should be an option to generate a Tech-Support file in the Web management application, and there is not.

Workaround: Generate this file using the CLI command. To do this using TFTP transfer, use the following command syntax.

```
Host_zl_Switch# wireless-services <slot id >
```

```
Host_zl_Switch(wireless-services-slot)# support copy tech-support tftp://<ip address of tftp server>/<filename.tar.gz>
```

Applet (41536) — In the Web management interface L3 mobility page, changes made to the settings take affect without the user hitting the **Apply** button.

Workaround: Use **caution** - do not click an option that you do not intend to configure on this screen.

Applet (40012) — In the Web management interface Special Features -> Station Intrusion Detection, clicking in any of the threshold value fields enables the **Apply** button, even when no changes were made. If the user has a concern that they inadvertently made a change, the **Revert** button may be used.

Applet (41721) — The Web management interface produces a Java console error message when a DDNS TTL value of 1 is configured for a DHCP pool. Additionally, the value does not get saved to the running configuration.

Workaround: Though a DDNS TTL value of 1 would be an unusual setting, if the user desires this setting, reconfiguring it a second time will allow the value to be saved.

Applet (1000460321) — The Web management interface Security -> MAC Filters -> Authentication column has a "#" in place of MAC-Auth.

Applet (1000460349) — The Web management interface Help section for the Security -> NAT -> Configuration page states that the "list is empty".

Chassis (40367) — The switch does not consistently report the correct module status after execution of the **halt** command. Typing **show wireless-services <slot-id>** at the switch CLI after the **halt** has been executed may show a status of "not responding" even though the module has been successfully shut down. It is safe to remove the module in that circumstance.

Chassis (41075) — The chassis self test LED should not be extinguished until the module is fully booted and ready. It currently shuts off early.

CLI (40764) — It is possible to configure a duplicate SSID (an invalid condition) using the CLI.

Workaround: Configure SSIDs via the Web management interface or validate your configuration by examination after CLI use.

CLI (41227) — The CLI allows the user to enter the command to remove an access-group that does not exist without producing an error message.

CLI (40893) — The sFlow timeout values that can be configured via the CLI differ from those considered valid by the Web management interface. This does not have any significant consequence; values configured in either management context will be honored.

CLI (38053) — There is no support for tethereal on the module.

Workaround: Use the local or remote mirroring features of the switch to perform packet captures.

Infrastructure (41648) — The Web management interface does not display the management interface IP address for layer 3 mobility when the **no layer3-mobility local address** command is executed through the CLI. Although the CLI output to the **show layer3-mobility global** command correctly displays the management VLAN interface as the "local address", the Web management interface continues to display the local interface IP address.

Workaround: View the configuration using the CLI if there is some question about the active configuration.

Infrastructure (39772) — When the primary RADIUS server is unavailable, a valid secondary RADIUS server configuration will successfully authenticate the wireless client, though the error messages generated may mislead the network administrator into thinking authentication did not occur. Syslog messages may be similar to the following (date, time and IP stamps were removed for clarity).

```
%USER-3-ERR: WIOS_SNMP[981]:auth failed:user manager role 0 src 0
%IMI-5-AUTHNOTIFY: Radius server secret not configured or server not reachable. Hence
trying next auth method
%PM-4-PROCNORESP: Process "fileMgmt" is not responding (2/20)
%PM-4-PROCNORESP: Process "securitymgr" is not responding (1/20)
%PM-4-PROCNORESP: Process "radconfd" is not responding (2/20)
%PM-4-PROCNORESP: Process "leaseparsed" is not responding (1/20)
%PM-4-PROCNORESP: Process "imi" is not responding (2/20)
%PM-4-PROCNORESP: Process "ccstatsd" is not responding (2/20)
```

```
%PM-4-PROCNORESP: Process "isDiag" is not responding (2/20)
%PM-4-PROCNORESP: Process "snmpd" is not responding (2/20)
%PM-4-PROCNORESP: Process "fileMgmt" is not responding (1/20)
%PM-4-PROCNORESP: Process "radconfd" is not responding (1/20)
%PM-4-PROCNORESP: Process "imi" is not responding (1/20)
%PM-4-PROCNORESP: Process "ccstatsd" is not responding (1/20)
%PM-4-PROCNORESP: Process "isDiag" is not responding (1/20)
%PM-4-PROCNORESP: Process "snmpd" is not responding (1/20)
%USER-5-NOTICE: WIOS_SNMP[961]: user ezhil login
```

Infrastructure (39875) — Alternate (secondary) methods of user login are designed to function when the primary method is unreachable - not when the primary method fails.

Infrastructure (41564) — The Img-File-Ver parameter in the CLI and the corresponding Management -> System Maintenance -> Update Server -> Software version parameter of the Web management application are not required values, and they should be. The image file will not be pulled if the version is empty, even if the force-upload parameter is set.

Infrastructure (39890) — Neither the CLI nor the Web management interface allow a domain name string of more than 70 characters in the DHCP server scope configuration.

Infrastructure (40734) — System administrators logged in with operator privileges are not able to execute the **show run** command at the CLI.

Workaround: view the running configuration from the Web management interface.

Infrastructure (41442) — A socket error may be produced during use of the update server function, though the feature is not affected by the error.

Infrastructure (1000459250) — VLAN statistics are not counting properly; both the Web management interface and CLI and under reporting inbound and outbound utilization.

L2-L3 (41762) — If a DHCP scope is configured on a VLAN that does not have an IP address, the module will have to be restarted after the IP address is assigned to the VLAN in order to allow the DHCP functionality to initialize properly.

Best Practice: Configure interfaces first, then configure the services that will be used by the interfaces.

L2-L3 (40778) — The Web management interface allows duplicate IP addresses to be set for the DNS server, the default router, and the Netbios server settings. The CLI, given the same parameters, appropriately triggers an error.

Best Practice: Review the running- or startup-config files for the validity of the IP addresses if problems are encountered.

L2-L3 (38070) — The user is able to configure a DHCP excluded address that is already in use by the static DHCP pool.

Workaround: Configure the DHCP range and exclusions prior to activating the DHCP server.

L2-L3 (39840) — A second default gateway configuration will not overwrite the originally configured value, but will be ignored.

Workaround: Remove the default gateway address prior to configuring a new address.

L2-L3 (41737) — Attaching an IP ACL with an *allow any* ACE to the downlink port stops all the traffic on the downlink, even if there is a MAC extended ACL to explicitly allow ARPs.

Workaround: ACLs attached to the downlink port need to explicitly allow the radio port traffic to get through to the module, as shown by a portion of a **show run** command below.

```
ip access-list extended 100
 permit ip any any rule-precedence 1
mac access-list extended 200
```

```
permit any any type arp rule-precedence 1
permit any any type 34691 rule-precedence 2
!
interface dnlink
ip access-group 100 in
mac access-group 200 in
```

L2-L3 (41469) — The error message, "ERROR: There must be at least one peer in established state to execute this command" is always displayed when doing a reload from within the module CLI redundancy context, even when peers are present.

Workaround: Execute the **reload** command from either the Web management interface, or the module CLI.

L2-L3 (40107) — DHCP boot file names are limited to 63 characters in both the CLI and the Web management interface.

L2-L3 (40163) — The DHCP hostname field is unable to accept non-alphanumeric characters.

Redundancy (41949) — A wireless station may show up on multiple modules in a redundancy group after failing over from a module that was removed from the switch. Connectivity and traffic for the wireless station are not affected.

Workaround: The genuine current wireless station owner is the one with the shortest amount of time in the "Last Active" field in the Device Information -> Wireless Stations -> Details button.

Security (36833) — The integrated firewall feature is supported only for packets received on Layer 3 interfaces. For packets getting switched, no firewall protection is applied. The firewall functionality supports protection against various network level attacks and inspects each packet for possible corruption that can indicate some kind of attack.

Security (41086) — The ACL logging functionality is not available for Layer 2 or WLAN ACLs.

Security (39537) — FTP control packets are not getting appropriately marked when a standard access list is configured for marking TOS bits.

Security (1000460306) — MAC filter rules are designed to apply to the association process. If a wireless station is already associated, a new "deny" MAC filter configured through Security -> MAC Filter in the Web management interface does not take effect until the station re-associates. If the administrator wants the filter to take effect immediately, the wireless station should be disconnected via Device Information -> Wireless Stations -> Disconnect. Rules configured in the latter context take effect immediately.

Security (1000460347) — Adding a MAC Filter via the Web management interface (Device Information -> Wireless Stations -> Disconnect screen) only associates the rule to WLANs 1-64.

SNMP (39709) — Configuration options that have been initiated but not saved in the CLI context cannot be edited via the Web management interface. An "SNMP Exception" message will occur with the failure.

Workaround: Save any changes made in the CLI from the CLI prior to attempting to edit them through the Web management interface.

SNMP (40513) — An SNMP timeout occurs when a DHCP option value containing more than 100 characters is entered in the DHCP pool configuration.

Workaround: Keep the configuration of option values to 100 characters or less.

SNMP (39823) — An SNMP timeout error may occur while generating a 2048 byte RSA key for use with a certificate.

Workaround: Confirm that the key was not generated; sometimes the key gets generated but a false error message is produced. If the key was not generated, retrying key generation should resolve the issue.

SNMP (41053) — The dynamic DHCP bindings viewed in the Web management interface display the expiration time in GMT rather than accurately reflecting the configured time zone offset.

Workaround: The expiration time is properly displayed in the output for the CLI command, **show ip dhcp binding**.

SNMP (37189) — The module does not support “noAuthnoPriv” and “AuthnoPriv” security levels for SNMPv3 users, but the CLI supports the commands for setting those levels.

Workaround: Configure SNMPv3 through the Web management interface, which appropriately allows only the “AuthPriv” security level.

SNMP (40001) — The SNMP port number for configuration of the trap destination is a optional parameter in the CLI, while it is a mandatory parameter in Web management interface. The module administrator should use the configuration interface that best meets their needs.

Wireless (40983) — Rate limiting is not applied to wireless stations that have roamed or have reconnected to the network if cached PMK is configured.

Workaround: Disable PMK caching when vendor specific attributes are required for rate limiting a wireless client (e.g. when using IDM). PMK caching is a default WPA2 value, and may be disabled in the Web management interface using Network Setup -> WLAN Setup -> Edit -> WPA/WPA2 -> Fast Roaming -> and uncheck PMK Caching.

Wireless (41726) — Setting the country code after Rogue AP detection is enabled may cause the module to reset continuously. This is an unlikely scenario since the country code must be set prior to the module's ability to adopt radio ports and is unlikely to require a second configuration. Best Practice: Set the country code prior to configuring the module.

Workaround: Disable Rouge AP detection prior to re-configuring the country code.

Release WT.01.10

ESPD — When PMK caching is enabled, and a client using WPA/WPA2 disconnects and ages out of the table, log messages like the following may be seen (date, time, severity, and IP address stamps removed for clarity).

```
espd: ESPd_emi_req() - Invalid OpCode
```

(Note: This issue has been resolved. See [“Release WT.01.16” on page 19](#) under “Software Fixes”.

Release WT.01.13

Release WT.01.13 is a *special* release for WESM zl modules purchased prior to April 1, 2008, in the European Union and selected countries/regions. For more information, see [“Release WT.01.13” on page 14](#).

Infrastructure (14207) — The wireless interface counter statistics displayed are incorrect; the tx_retries counter may increment interfaces where a radio port is not attached.

Infrastructure (45508) — The network time protocol (NTP) clock stratum displays a value of 5 irrespective of the configured value.

Infrastructure (45760) — When logging level 7 is enabled with output to monitor, and debug all is given as a parameter, the module management will become unresponsive after exiting the CLI. This may also be associated with a kernel panic and creation of probetabled core files.

Security (45714) — MAC authentication with the local RADIUS server will fail if the MAC address is provided in a paired-colon format.

Security (45715) — Web authentication with the local RADIUS server will fail if the username contains a colon.

Security (45550) — When the local RADIUS server has the maximum number of clients, and an attempt is made to add another client, the error message displayed is “Error:Maximum proxy realm configured” rather than “Error:Maximum client config reached”.

Release WT.01.28

Infrastructure (PR_41333) — When log level is set higher than level 5, the log message below will constantly be logged to syslog. The heavy log activity increases demand for CPU resources, which could result in WESM stability problems.

Log message, "%KERN-6-INFO: wtc-action (2) ..."

Technology for better business outcomes

To learn more, visit www.hp.com/go/procurve/

© Copyright 2009-2010 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP will not be liable for technical or editorial errors or omissions contained herein.



May 2010

Manual Part Number
5991-8624